

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of :  
Toshihisa NAKANO et al. :  
Serial No. NEW : **Attn: APPLICATION BRANCH**  
Filed March 18, 2004 : Attorney Docket No. 2004\_0442A

RECORDING APPARATUS AND CONTENT  
PROTECTION SYSTEM

**CLAIM OF PRIORITY UNDER 35 USC 119**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450


Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2003-081467, filed March 24, 2003, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Toshihisa NAKANO et al.

By   
Michael S. Huppert  
Registration No. 40,268  
Attorney for Applicants

MSH/kjf  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
March 18, 2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    3 月 2 4 日  
Date of Application:

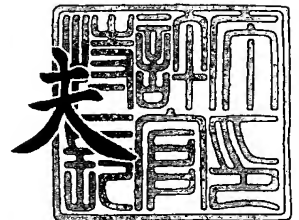
出 願 番 号                      特 願 2 0 0 3 - 0 8 1 4 6 7  
Application Number:  
[ST. 10/C]:                      [ J P 2 0 0 3 - 0 8 1 4 6 7 ]

出      願      人                      松 下 電 器 産 業 株 式 有 限 公 司  
Applicant(s):

2 0 0 3 年 1 2 月 1 2 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



出証番号    出証特 2 0 0 3 - 3 1 0 3 5 1 6

【書類名】 特許願

【整理番号】 2022550101

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 中野 稔久

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 布田 裕一

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 大森 基司

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 原田 俊治

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【電話番号】 06-4806-7530

## 【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

## 【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0213583

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 記録装置及び著作権保護システム

【特許請求の範囲】

【請求項 1】 デジタル著作物であるコンテンツを記録媒体に記録する記録装置であって、

外部から提供されるコンテンツを取得するコンテンツ取得手段と、

受信されたコンテンツの種別を特定するコンテンツ種別特定手段と、

前記記録媒体の種別を特定する記録媒体種別特定手段と、

前記コンテンツ種別特定手段で特定されたコンテンツの種別と前記記録媒体種別特定手段で特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも 1 つの記録方式を選択する記録方式選択手段と、

選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録手段と

を備えることを特徴とする記録装置。

【請求項 2】 前記コンテンツ種別特定手段は、前記コンテンツの種別として、少なくとも、前記コンテンツが伝送媒体によって提供された第 1 種別か、記録媒体によって提供された第 2 種別かを特定する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 3】 前記記録媒体種別特定手段は、前記記録媒体の書き換え不可領域に予め格納されている情報の種類によって、前記記録媒体の種別を特定することを特徴とする請求項 1 記載の記録装置。

【請求項 4】 前記記録方式選択手段は、コンテンツの著作権を保護する方式に対応した複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 5】 前記記録方式選択手段は、さらに、前記コンテンツを提供した提供元からの指示に基づいて、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 6】 前記コンテンツには、前記複数の記録方式の中の 1 つを指定

する指定情報が含まれ、

前記記録方式選択手段は、さらに、前記コンテンツに含まれる指定情報に基づいて、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 7】 前記記録方式選択手段は、さらに、ユーザの指示に基づいて、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 8】 前記記録方式選択手段は、さらに、前記コンテンツに要求されるセキュリティレベルに基づいて、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 9】 前記記録方式選択手段は、さらに、前記コンテンツの品質に基づいて、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 10】 前記コンテンツ取得手段は、取得するデータの種類に対応した複数の入力チャネル部を有し、

前記記録方式選択手段は、さらに、前記コンテンツが前記複数の入力チャネル部のいずれの入力チャネル部で取得されたかによって、前記複数の記録方式の中から 1 つの記録方式を選択する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 11】 前記記録手段は、前記記録媒体に第 1 の記録方式で第 1 のコンテンツが記録されている場合には、前記第 1 のコンテンツを残したまま、第 2 のコンテンツを第 2 の記録方式で記録する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 12】 前記記録媒体には、第 1 の記録方式で第 1 のコンテンツが記録され、

前記記録装置は、さらに、前記記録媒体から前記第 1 のコンテンツを読み出した後に、当該第 1 のコンテンツを第 2 の記録方式で前記記録媒体に記録する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 13】 前記記録方式選択手段は、前記複数の記録方式の中から 2 以上の記録方式を選択し、

前記記録手段は、選択された 2 以上の記録方式に従って前記記録媒体に前記コンテンツを記録する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 14】 前記コンテンツ取得手段は、取得したコンテンツを、伝送路を介して前記記録手段に送信し、

前記記録手段は、前記伝送路を介して受信したコンテンツを前記記録媒体に記録し、

前記コンテンツ取得手段は、前記コンテンツを、送信先となる記録手段が採用する記録方式に従って暗号化した後に、当該暗号化コンテンツを前記記録手段に送信する

ことを特徴とする請求項 1 記載の記録装置。

【請求項 15】 前記記録方式には、コンテンツの著作権を保護する方式に対応した第 1 及び第 2 の記録方式が含まれ、

前記コンテンツ取得手段は、前記記録手段が前記第 1 の記録方式を採用している場合には、予め保持する秘密鍵を用いて前記コンテンツを暗号化し、前記記録手段が前記第 2 の記録方式を採用している場合には、外部から取得した秘密鍵を用いて前記コンテンツを暗号化する

ことを特徴とする請求項 14 記載の記録装置。

【請求項 16】 前記記録方式には、コンテンツの著作権を保護する方式に対応した第 1 及び第 2 の記録方式が含まれ、

前記コンテンツ取得手段は、取得したコンテンツが前記第 1 の記録方式に対応した暗号化コンテンツである場合には、当該コンテンツを前記第 2 の記録方式に対応した暗号化コンテンツに再暗号化した後に前記記録手段に送信する

ことを特徴とする請求項 14 記載の記録装置。

【請求項 17】 伝送路を介して接続されたサーバ装置と端末装置とから構成される著作権保護システムであって、

前記サーバ装置は、

暗号化コンテンツを当該暗号化コンテンツを復号化するのに必要な復号化情報とが記録された記録媒体から前記暗号化コンテンツ及び前記復号化情報を読み出す読み出し手段と、

読み出された暗号化コンテンツ及び復号化情報を前記伝送路を介して前記端末装置に送信する送信手段とを備え、

前記端末装置は、

前記伝送路を介して送信されてくる暗号化コンテンツ及び復号化情報を受信する受信手段と、

受信された暗号化コンテンツを受信された復号化情報を用いて復号化する復号化手段とを備え、

前記送信手段は、前記端末装置との間でセキュアな伝送チャネルを確立した後に、当該伝送チャネルを介して前記復号化情報を送信する

ことを特徴とする著作権保護システム。

【請求項 18】 前記復号化情報には、前記記録媒体の書き換え不可領域に格納されていた当該記録媒体を特定する媒体識別情報が含まれる

ことを特徴とする請求項 17 記載の著作権保護システム。

【請求項 19】 前記端末装置は、さらに、前記復号化手段によって復号化されたコンテンツを音及び画像の少なくとも 1 つとして再生する再生手段を備える

ことを特徴とする請求項 17 記載の著作権保護システム。

【請求項 20】 前記端末装置は、さらに、前記復号化手段によって復号化されたコンテンツを記録媒体に記録する記録手段を備える

ことを特徴とする請求項 17 記載の著作権保護システム。

【請求項 21】 前記記録手段は、前記復号化手段によって復号化されたコンテンツを当該復号化に対応する暗号化とは異なる暗号化方式で暗号化した後に、前記記録媒体に記録する

ことを特徴とする請求項 20 記載の著作権保護システム。

【請求項 22】 伝送路を介してサーバ装置と接続される端末装置であって



前記サーバ装置は、

暗号化コンテンツを当該暗号化コンテンツを復号化するのに必要な復号化情報とが記録された記録媒体から前記暗号化コンテンツ及び前記復号化情報を読み出す読み出し手段と、

読み出された暗号化コンテンツ及び復号化情報を前記伝送路を介して前記端末装置に送信する送信手段とを備え、

前記端末装置は、

前記伝送路を介して送信されてくる暗号化コンテンツ及び復号化情報を受信する受信手段と、

受信された暗号化コンテンツを受信された復号化情報を用いて復号化する復号化手段とを備え、

前記送信手段は、前記端末装置との間でセキュアな伝送チャネルを確立した後に、当該伝送チャネルを介して前記復号化情報を送信する

ことを特徴とする端末装置。

【請求項 23】 デジタル著作物であるコンテンツを記録媒体に記録する記録方法であって、

外部から提供されるコンテンツを取得するコンテンツ取得ステップと、

受信されたコンテンツの種別を特定するコンテンツ種別特定ステップと、

前記記録媒体の種別を特定する記録媒体種別特定ステップと、

前記コンテンツ種別特定ステップで特定されたコンテンツの種別と前記記録媒体種別特定ステップで特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも 1 つの記録方式を選択する記録方式選択ステップと、

選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録ステップと

を備えることを特徴とする記録方法。

【請求項 24】 伝送路を介して接続されたサーバ装置と端末装置とから構成される著作権保護システムに用いる記録方法であって、

前記サーバ装置は、

暗号化コンテンツを当該暗号化コンテンツを復号化するのに必要な復号化情報

とが記録された記録媒体から前記暗号化コンテンツ及び前記復号化情報を読み出す読み出しステップと、

読み出された暗号化コンテンツ及び復号化情報を前記伝送路を介して前記端末装置に送信する送信ステップとを備え、

前記端末装置は、

前記伝送路を介して送信されてくる暗号化コンテンツ及び復号化情報を受信する受信ステップと、

受信された暗号化コンテンツを受信された復号化情報を用いて復号化する復号化ステップとを備え、

前記送信ステップにおいては、前記端末装置との間でセキュアな伝送チャネルを確立した後に、当該伝送チャネルを介して前記復号化情報を送信する

ことを特徴とする記録方法。

【請求項 25】 デジタル著作物であるコンテンツを記録する記録装置により記録される記録媒体であって、

前記記録装置は、

外部から提供されるコンテンツを取得するコンテンツ取得手段と、

受信されたコンテンツの種別を特定するコンテンツ種別特定手段と、

前記記録媒体の種別を特定する記録媒体種別特定手段と、

前記コンテンツ種別特定手段で特定されたコンテンツの種別と前記記録媒体種別特定手段で特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも 1 つの記録方式を選択する記録方式選択手段と、

選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録手段とを備える

ことを特徴とする記録媒体。

【請求項 26】 デジタル著作物であるコンテンツを記録媒体に記録する記録方法に用いるプログラムであって、

外部から提供されるコンテンツを取得するコンテンツ取得ステップと、

受信されたコンテンツの種別を特定するコンテンツ種別特定ステップと、

前記記録媒体の種別を特定する記録媒体種別特定ステップと、

前記コンテンツ種別特定ステップで特定されたコンテンツの種別と前記記録媒体種別特定ステップで特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも1つの記録方式を選択する記録方式選択ステップと、

選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録ステップと

を備えることを特徴とするプログラム。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを、光ディスク等の記録媒体に記録する際に用いられる記録装置及び著作権保護システム（CPS：Content Protection System）に関し、特に複数の著作権保護記録方式に対応可能な記録装置及び著作権保護システムに関する。

##### 【0002】

#### 【従来の技術】

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツ（以下、コンテンツ）を生成して、光ディスク等の大容量記録媒体に格納して配布する、あるいはネットワークを介して配布するシステムが現れている。配布されたコンテンツは、記録装置を用いてDVD等の記録媒体に記録される対象となり、コンピュータや再生装置等で読み出されて、再生の対象となる。

##### 【0003】

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピー等といった不正利用を防止するために暗号化技術が用いられ、このコンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。

##### 【0004】

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを実現する技術を鍵無効化技術と呼ばれる（例えば、特許文献1参照）。

#### 【0005】

図12は、鍵無効化技術を説明するための説明図である。この鍵無効化技術による著作権保護システムは、記録媒体1201の書き込み不可領域1201aに媒体固有情報（MID:Media ID）1203及び鍵無効化データ（KRD:Key Revocation Data）1202が書き込まれていることを特徴とする。

#### 【0006】

図12において、光ディスク等の記録媒体1201は、書き換え不可領域1201aと書き換え可能領域1201bを有している。この書き換え不可領域1201aは、読み込みのみが可能な領域であり、鍵無効化データ（KRD）1202及び媒体固有番号（MID）1203が記録されている。また、書き換え可能領域1201bには、暗号化コンテンツ鍵1204と暗号化コンテンツ1205が記録されている。

#### 【0007】

通常の状態であれば、再生装置等の機器1（1206）は、記録媒体1201に記録されている暗号化コンテンツの利用を行うために、機器固有のデバイス鍵1（Devkey1）を用いて暗号文（E）を復号化してメディア鍵（MK）を得て、このメディア鍵（MK）を用いて暗号化コンテンツ鍵1204の暗号文を復号化してコンテンツ鍵（CK）を取得して、このコンテンツ鍵（CK）を用いて暗号化コンテンツ1205を復号化することによりコンテンツ（content）の再生を行うことができる。

#### 【0008】

そして、例えば機器2に対応するデバイス鍵2（Devkey2）が不正者によって

暴露された場合においては、鍵無効化データ 1202 における暗号文 (E) を復号化しても正規のメディア鍵 (MK) は取得できず、無効化されたデータ (x x x) しか取得できない。このため、機器 2 は正規のコンテンツ鍵 (CK) を復号化することができず、不正にコンテンツの利用を図ることができない。

#### 【0009】

このように、著作権保護システムである鍵無効化技術においては、復号化に用いる鍵 (本図においてはデバイス鍵 2) を鍵無効化データ 1202 を用いて無効化することにより、コンテンツの不正使用の防止を図る。

#### 【0010】

一方、光ディスク等の記録媒体に記録されているコンテンツの読み出し、あるいは書き込みは、光ディスクドライブと称されるパソコン周辺機器で行われることが一般的であるが、機器の互換性を達成するためにその入出力の方法は公開の情報として標準化され、秘密にされないことが一般的である。このため、記録媒体に記録されているコンテンツは、パソコン等により、容易に読み出すことが可能であり、また、読み出したデータを他の記録媒体に書き込むことも容易である。したがって、コンテンツの著作権を保護するシステムにおいては、記録媒体上のデータを読み出し、他の記録媒体に書き込むという、通常のユーザが行い得る行為に対して、それを防止する有効な機能を備えるシステムでなければならない。そのような目的を達成する技術として、個々の記録媒体に関連づけてコンテンツを記録することによってコンテンツの複製を防止するいわゆるメディアバインドと呼ばれる技術がある (例えば、特許文献 2 参照)。このメディアバインド技術は、記録媒体の書き換え不可領域に記録されている媒体固有番号 (MID) を用いてコンテンツの暗号化を行う技術である。

#### 【0011】

そして、前記鍵無効化技術、或いは前記メディアバインド技術の機能を有する著作権保護システムの具体例としては、DVD-RAM 等で使用されている CPRM (Content Protection for Recordable Media) 記録方式がある。

#### 【0012】

そして、従来、著作権保護システムとして CPRM 記録方式のみに対応する記

録装置は存在する。図13は、従来の単一の著作権保護システムに対応する記録装置1301の説明図である。

#### 【0013】

記録装置1301は、放送、DVD等からコンテンツを受信して、記録メディア1303等にコンテンツを記録するための装置であり、記録方式選択部1302を備えている。この記録方式選択部1302は、著作権の保護を図るために著作権保護コンテンツ（CPコンテンツ）又は著作権保護を必要としないコンテンツ（Non-CPコンテンツ）というソースの種類、記録メディア1303及び1304の種類に応じてCPRM記録方式でコンテンツの記録を行うか否かの選択を行う。

#### 【0014】

記録方式選択部1302は、ソースの種類に応じて記録方式を選択するものであり、コンテンツが著作権保護を必要とするコンテンツである場合には、CPRM記録方式を選択し、著作権保護を必要としないコンテンツである場合には、Non-CP記録方式を選択する。

#### 【0015】

また、記録方式選択部1302は、記録メディア1303等の種類に応じて記録方式の選択を行う。記録メディア1303には、媒体固有番号（MID）及び鍵無効化データ（KRD）が書き込まれているため、記録方式選択部1302は、CPRM記録方式か著作権保護を行わないNon-CP記録方式でコンテンツの記録を行うかの選択を行う。

#### 【0016】

また、記録メディア1304は、媒体固有情報（MID）及び鍵無効化データ（KRD）が書き込まれていないため、記録方式選択部1302は、著作権保護を行わないNon-CP記録方式でコンテンツの記録を行うことを選択する。尚、記録装置1301から記録メディアへのコンテンツの記録不可の場合をNGとする。

#### 【0017】

#### 【特許文献1】

特開 2002-281013 号公報

【0018】

【特許文献 2】

特許第 3073590 号公報

【0019】

【発明が解決しようとする課題】

近年のデジタル技術の進歩に伴い、上述のようにコンテンツ配信における著作権保護システムも前記のような従来の著作権保護システムとは別の複数の著作権保護システムの導入が予定されている。このような状況において、記録装置及び再生装置は、上述した CPRM 記録方式等の従来型の著作権保護システム以外の新たな著作権保護システムに対応する必要がある。すなわち、従来型の著作権保護システム及び新たな著作権保護システムという複数の著作権保護システムに対応可能な記録装置が要求される。

【0020】

しかしながら、上述した従来の記録装置 1301 は、例えば CPRM 記録方式という単一の著作権保護記録方式に対応する記録装置であり、現状の著作権保護システム、及び今後導入される新たな著作権保護システムに対応する複数の著作権保護記録方式に対応できる記録装置は存在しない。

【0021】

ところで、再生装置においては、従来より複数の著作権保護システムに対応する再生装置は存在する。具体的には、現在の DVD-RAM レコーダーは著作権保護システムである CSS 記録方式と CPRM 記録方式との両方をサポートしてコンテンツの再生を行うことが可能である。

【0022】

そして、著作権保護システムの高度化に伴い 1 枚のディスクで複数の著作権保護システムに対応するマルチディスクの登場が予測される。しかし、従来のディスクは単一の著作権保護システムに対応するディスクであり、複数の著作権保護システムに対応するマルチディスクを利用したサーバ装置と記録装置との間のコンテンツの移動やコピーを実現する著作権保護システムは存在しない。

**【0023】**

さらに、家庭内ネットワークの普及に伴い家庭内でのコンテンツの移動やコピーを実現する仕組みが確立されつつある状況下においてコンテンツ配信における更なる著作権保護の要望もある。

**【0024】**

本発明は、前記課題を解決するためのものであり、コンテンツを記録媒体に記録する記録装置において、従来型の著作権保護システムに対応するのみでなく、複数の新たな著作権保護システムに対応可能な記録装置を提供することを第一の目的とする。

**【0025】**

また、第二の目的として、複数の著作権保護記録方式が存在する場合において、コンテンツの配信先である記録装置の機能、コンテンツが記録される記録メディアの種類に応じて、サーバ装置からのコンテンツの配信を効率的に行う著作権保護システムを提供することを目的とする。

**【0026】****【課題を解決するための手段】**

前記課題を解決するために、本発明は、デジタル著作物であるコンテンツを記録媒体に記録する記録装置であって、外部から提供されるコンテンツを取得するコンテンツ取得手段と、受信されたコンテンツの種別を特定するコンテンツ種別特定手段と、前記記録媒体の種別を特定する記録媒体種別特定手段と、前記コンテンツ種別特定手段で特定されたコンテンツの種別と前記記録媒体種別特定手段で特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも1つの記録方式を選択する記録方式選択手段と、選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録手段とを備えることを特徴とする。

**【0027】**

また、前記課題を解決するために、本発明は、伝送路を介して接続されたサーバ装置と端末装置とから構成される著作権保護システムであって、前記サーバ装置は、暗号化コンテンツを当該暗号化コンテンツを復号化するのに必要な復号化情報とが記録された記録媒体から前記暗号化コンテンツ及び前記復号化情報を読



み出す読み出し手段と、読み出された暗号化コンテンツ及び復号化情報を前記伝送路を介して前記端末装置に送信する送信手段とを備え、前記端末装置は、前記伝送路を介して送信されてくる暗号化コンテンツ及び復号化情報を受信する受信手段と、受信された暗号化コンテンツを受信された復号化情報を用いて復号化する復号化手段とを備え、前記送信手段は、前記端末装置との間でセキュアな伝送チャネルを確立した後に、当該伝送チャネルを介して前記復号化情報を送信することを特徴とする。

#### 【0028】

尚、本発明は、上述のような記録装置として実現できるのみではなく、この記録装置が備える手段をステップとする記録方法、また、当該記録方法をコンピュータ等で実現させるプログラムとして実現したり、当該プログラムを光ディスク、CD-ROM等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

#### 【0029】

##### 【発明の実施の形態】

以下、本発明の実施の形態に係る記録装置及び著作権保護システムについて図面を用いて説明する。

#### 【0030】

##### (実施の形態)

最初に、上述した従来のCPRM記録方式と異なる本実施の形態に係る著作権保護システムに用いるCPS-2記録方式について説明する。このCPS-2記録方式は、記録媒体固有の番号である媒体固有番号(MID)から認証子(MAC)を生成することを特徴とする。

#### 【0031】

図1は、本実施の形態に用いる著作権保護システムに用いるCPS-2記録方式の全体構成を示す概略図である。図1には、光ディスク等の記録媒体120に記録を行う記録装置100の構成を示すブロック図、記録装置100から記録媒体120に記録される情報、及び記録媒体120を用いてコンテンツの再生を行う再生装置200の構成を示すブロック図が示され、各処理部の関係が矢印で示

されている。

### 【0032】

記録装置100は、各記録装置100が秘密に保有するデバイス鍵を格納するデバイス鍵格納部101と、鍵無効化データ（HKB）を鍵無効化データ配信局130より取得して格納する鍵無効化データ格納部102と、鍵無効化データをデバイス鍵で復号してメディア鍵（Km）を算出するメディア鍵計算部103と、メディア鍵計算部103において計算したメディア鍵（Km）と暗号化コンテンツ鍵と媒体固有番号（MID）とを一方方向性関数に入力して認証子（MAC：Message Authentication Code）を生成する認証子生成部104と、算出したメディア鍵（Km）で外部から入力されたコンテンツ鍵を暗号化するコンテンツ鍵暗号化部105と、コンテンツ鍵で外部から入力されたコンテンツを暗号化するコンテンツ暗号化部106と、公開鍵暗号系における秘密鍵を格納する秘密鍵格納部107と、前記秘密鍵に対応する公開鍵に対して認証局（以下、CAと記す）による署名が付与された証明書を格納する証明書格納部108と、CRL配信局140より配信される最新の無効化した証明書の一覧を示す公開鍵証明書無効化リスト（CRL：Certification Revocation List）を格納するCRL格納部109と、前記メディア鍵に対する署名を生成する署名生成部110とを備える。本実施に形態に係る著作権保護システムにおいて、認証子（MAC）は、再生装置200においてコンテンツの正当性を判定する際に用いる情報である。

### 【0033】

また、記録媒体120は、書き換え不可領域（二重括弧に示す領域）に媒体固有番号を記録する媒体固有番号記録領域121を有し、書き換え可能領域には、記録装置100が暗号化に使用した鍵無効化データを記録する鍵無効化データ記録領域122と、暗号化したコンテンツ鍵を記録する暗号化コンテンツ鍵記録領域123と、暗号化したコンテンツを記録する暗号化コンテンツ記録領域124と、記録装置100が生成した署名を記録する署名記録領域125と、記録装置100が保有するCRL、並びに証明書を記録するCRL記録領域126及び証明書記録領域127と、認証子生成部104において生成された認証子を記録する認証子記録領域128とを有する。本実施の形態においては、記録媒体120

は、媒体固有番号記録領域 121 のみが書き換え不可領域に書き込まれ、その他の情報は書き換え可能領域に書き込まれている。このため、CPS-2 記録方式においては、鍵無効化データを記録媒体 120 の書き込み可能領域である鍵無効化データ記録領域に書き込むことが可能となる。

#### 【0034】

再生装置 200 は、各装置が秘密に保有するデバイス鍵を格納するデバイス鍵格納部 201 と、記録媒体 120 から読み出した鍵無効化データをデバイス鍵で復号してメディア鍵 (Km) を算出するメディア鍵計算部 202 と、メディア鍵計算部 202 で取得するメディア鍵 (Km)、記録媒体 120 の媒体固有番号記録領域 121 より取得する媒体固有番号、及び記録媒体 120 の暗号化コンテンツ鍵記録領域 123 に記録されている暗号化コンテンツ鍵の 3 つの情報を用いて一方向性の関数に従って認証子の生成を行う認証子生成部 203 と、算出したメディア鍵で記録媒体 120 から読み出した暗号化コンテンツ鍵を復号するコンテンツ鍵復号部 204 と、復号して得たコンテンツ鍵で記録媒体 120 から読み出した暗号化コンテンツを復号するコンテンツ復号部 205 と、CA の公開鍵を格納する CA 公開鍵格納部 206 と、CA の公開鍵を用いて記録媒体 120 から読み出した証明書の正当性を検証する、即ち証明書に付与された署名の検証を行う証明書検証部 207 と、CRL 配信局 140 から取得する最新の CRL を格納する CRL 格納部 208 と、CA の公開鍵を用いて記録媒体 120 から読み出した CRL の正当性を検証する、即ち CRL に付与された署名の検証を行う CRL 検証部 209 と、記録媒体 120 から読み出してその正当性を検証した CRL と、CRL 格納部 208 に格納する CRL の新旧を比較して、新しい CRL を CRL 格納部 208 に格納する CRL 比較／更新部 210 と、CRL 格納部 208 に格納する最新の CRL に記録媒体 120 から読み出した証明書が登録されているかを判定する証明書判定部 211 と、記録媒体 120 から読み出した署名を、同じく記録媒体 120 から読み出した証明書を使用して検証する署名検証部 212 と、種々の検証、並びに判定結果に基づいて制御されるスイッチ 213 とを備える。

#### 【0035】

さらに、再生装置 200 は、認証子生成部 203 より復号された認証子と、記録媒体 120 の認証子記録領域 128 に記録されている認証子とを比較する認証子比較部 214 を有する。この認証子比較部 214 は、認証子の比較結果をスイッチ 213 に伝えることにより、メディアを介した不正なコピーがされていないか、媒体固有番号 (MID) が正しい記録媒体に対してコンテンツが書き込まれているかの確認を行うことが可能となる。

#### 【0036】

このように、本実施の形態に係る著作権保護システムに用いる CPS-2 記録方式においては、記録装置 100 側において媒体固有番号 (MID) を用いて認証子 (MAC) を生成して、再送装置 200 側において認証子の比較を行うことによりコンテンツの不正使用の防止を図り、著作権保護を図ることが可能となる。

#### 【0037】

図 2 は、再生装置 200 の総数を  $n$  台として、2 台の再生装置 200 のデバイス鍵である DK\_\_3 及び DK\_\_4 が無効化されていると仮定した場合に、デバイス鍵 DK\_\_1 の再生装置 200 が記録した記録媒体 120 に格納されている各種データの具体例を示している。また、この例では、 $n$  台の再生装置 200 はそれぞれ固有のデバイス鍵を 1 つだけ保有している。尚、本図の記録媒体 120 においては、媒体固有番号記録領域 120a のみが書き換え不可領域となる。

#### 【0038】

(媒体固有番号記録領域 120a)

媒体固有番号記録領域 120a は、書き換え不可領域であり、記録媒体 120 ごとに、その記録媒体固有の番号 (MID) が記録されている。図 2 では、媒体固有番号は 16 進数 8 桁で表現されており、固有番号は「6」である。そして、この媒体固有番号 (MID) は記録媒体 120 の製造時において記録されるものであり、また、媒体固有番号 (MID) の先頭領域に記されている「0x」は媒体固有番号が 16 進数であることを示す。また、図 2 に例示している媒体固有番号は 32 ビットとなる。

#### 【0039】

(鍵無効化データ記録領域 120b)

鍵無効化データ記録領域 120b には、複数のデバイス鍵 (DK) で暗号化されたメディア鍵 (MK) が記録されている。ここで、 $E(X, Y)$  は、データ Y を鍵データ X で暗号化したときの暗号文を意味する記号として用いる。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、例えば DES 暗号などが使用される。また、再生装置 n が保有するデバイス鍵を DK\_\_n と表現している。

【0040】

図 2 では、DK\_\_3 及び DK\_\_4 の再生装置 200 が無効化されているため、それぞれが保有する DK\_\_3 及び DK\_\_4 では、メディア鍵 (MK) とは全く無関係のデータ「0」が暗号化されて記録されている。メディア鍵データをこのように生成することで、DK\_\_3 及び DK\_\_4 の再生装置 200 以外の全ての装置だけがメディア鍵 (MK) を共有でき、DK\_\_3 及び DK\_\_4 の再生装置 200 をシステムから排除することができる。なお、装置の無効化方法は他の方法を利用してよく、例えば、前記の特許文献 1 には木構造を利用した無効化方法が開示されている。

【0041】

(認証子記録領域 120c)

認証子記録領域 120c には、記録装置 100 の認証子生成部 104 において生成される認証子 (MAC) が記録されている。

【0042】

(暗号化コンテンツ鍵記録領域 120d)

暗号化コンテンツ鍵領域 120d には、メディア鍵 (MK) で暗号化されたコンテンツ鍵 (CK) が記録されている。

【0043】

(暗号化コンテンツ記録領域 120e)

暗号化コンテンツ記録領域に 120e は、コンテンツ鍵 (CK) で暗号化されたコンテンツが記録されている。

【0044】

(署名記録領域 120f)

署名記録領域 120f には、メディア鍵 (MK) と CRL に対して生成された署名が記録されている。ここで、 $\text{Sig}(X, Y)$  は、データ Y に対して鍵データ X を用いて生成した署名文を意味する記号として用いる。なお、使用される署名生成アルゴリズムは、公知の技術で実現可能であり、例えば、RSA 署名などが使用される。

【0045】

図 2 では、装置 1 の秘密鍵 ( $\text{SK}_{-1}$ ) を用いて生成された署名文が記録されている。

【0046】

(CRL 記録領域 120g)

CRL 記録領域 120g には、 $\text{DK}_{-1}$  の再生装置 200 が署名を生成するときに対象とした CRL が記録されている。CRL には、無効化すべき証明書 (ここでは  $\text{DK}_{-3}$  及び  $\text{DK}_{-4}$  の再生装置 200 の証明書) の ID が記載されており、それらに対する CA の署名が付与されている。なお、CA の署名は CRL の正当性を保証するためのものである。また、CRL のフォーマットは公知のものであっても、あるシステムに特化したものであってもよい。尚、ここで  $\text{ID}_{-3} \parallel \text{ID}_{-4}$  は、 $\text{DK}_{-3}$  及び  $\text{DK}_{-4}$  の再生装置 200 を一意に特定する ID の桁を連結することを示す。

【0047】

(証明書記録領域 120h)

証明書記録領域 120h には、 $\text{DK}_{-1}$  の再生装置 200 が署名を生成するときに用いた秘密鍵 ( $\text{SK}_{-1}$ ) に対応する証明書が記録されている。証明書には、証明書の ID、公開鍵 ( $\text{PK}_{-1}$ ) と、それらに対する CA の署名が付与されている。なお、CA の署名は証明書の正当性を保証するためのものである。また、証明書のフォーマットは公知のものであっても、あるシステムに特化したものであってもよい。

【0048】

次に、以上のような著作権保護システムに用いる CPS-2 記録方式における

記録装置 100、記録媒体 120、及び再生装置 200 のそれぞれにおける動作について説明する。

#### 【0049】

まず記録装置 100 における動作について説明すると、メディア鍵計算部 103 は、デバイス鍵格納部 101、並びに鍵無効化データ格納部 102 から、デバイス鍵、及び鍵無効化データをそれぞれ読み出し、メディア鍵データをデバイス鍵で復号することによりメディア鍵 (Km) を得る。

#### 【0050】

認証子生成部 104 は、媒体固有番号 (MID) と、メディア鍵計算部 103 で得たメディア鍵と、暗号化コンテンツ鍵とを一方向性関数に入力させることによって認証子 (MAC) を生成する。

#### 【0051】

コンテンツ鍵暗号化部 105 は、メディア鍵計算部 103 で計算されたメディア鍵で、外部から入力されたコンテンツ鍵を暗号化する。コンテンツ暗号化部 106 は、外部から入力されたコンテンツ鍵で、同じく外部から入力されたコンテンツを暗号化する。署名生成部 110 は、秘密鍵格納部 107 から秘密鍵を読み出し、メディア鍵、及び CRL に対する署名を生成する。

#### 【0052】

そして、記録装置 100 は、保有している鍵無効化データ、CRL、証明書、並びに生成した認証子、暗号化コンテンツ鍵、暗号化コンテンツ、署名を記録媒体 120 に記録する。

#### 【0053】

そして、再生装置 200 における動作について説明すると、再生装置 200 は、記録媒体 120 から、鍵無効化データ、媒体固有番号、認証子、暗号化コンテンツ鍵、暗号化コンテンツ、署名、CRL、証明書をそれぞれ読み出す。

#### 【0054】

メディア鍵計算部 202 は、デバイス鍵格納部 201 からデバイス鍵を読み出し、読み出した鍵無効化データを、デバイス鍵で復号することによりメディア鍵 (Km) を得る。

## 【0055】

認証子生成部203は、記録媒体120から読み出した媒体固有番号(MID)と、メディア鍵計算部202より得られるメディア鍵(Km)と、暗号化コンテンツ鍵とより認証子を復号する。認証子比較部214は、認証子生成部203より得られる認証子と記録媒体120より読み出される認証子の比較を行う。この比較の結果、認証子が一致する際には、認証子比較部214は、コンテンツの再生許可をスイッチ213に伝える。

## 【0056】

コンテンツ鍵復号部204は、記録媒体120より読み出した暗号化コンテンツ鍵を、メディア鍵計算部202より得られるメディア鍵(Km)で復号することによりコンテンツ鍵を得る。また、コンテンツ復号部205は、記録媒体120より読み出した暗号化コンテンツを、コンテンツ鍵復号部204で得たコンテンツ鍵で復号することによりコンテンツを得る。

## 【0057】

証明書検証部207は、CA公開鍵格納部206からCAの公開鍵を読み出し、記録媒体120の証明書記録領域127より読み出した証明書の正当性を、読み出したCAの公開鍵を用いて検証する。そして、証明書の正当性の検証がNGとなる場合はスイッチ213を開いてコンテンツを再生しない一方、証明書の正当性がOKの場合であり、スイッチ213を閉じてコンテンツを再生可能とする。尚、本発明においては、当該証明書検証部207、後述する証明書判定部211、署名検証部212、及び認証子比較部214の検証全てがOKの場合においてのみスイッチ213を閉じてコンテンツの再生を行う。

## 【0058】

CRL検証部209は、記録媒体120のCRL記録領域126より読み出したCRLの正当性を、CA公開鍵格納部206より読み出したCAの公開鍵を用いて検証する。

## 【0059】

CRL比較／更新部210は、CRL格納部208からCRLを読み出し、このCRLとCRL検証部209から読み出したCRLとの新旧を比較する。例え



ば、新旧の比較は、CRLに割り当てられているバージョン番号などを利用する。この比較した結果、新しいと判断したCRLをCRL格納部208に格納する。

#### 【0060】

証明書判定部211は、CRL格納部208からCRLを読み出し、記録媒体120より読み出した証明書が登録されているか否かを判定する。この判定で登録されている場合にはスイッチ213を開いてコンテンツを再生しない一方、登録されていない場合にはスイッチ213を閉じてコンテンツを再生可能とする。

#### 【0061】

署名検証部212は、記録媒体120の署名記録領域125より読み出した署名の正当性を、同じく記録媒体120より読み出した証明書と、CRL検証部209より読み出すCRLと、メディア鍵計算部202で生成したメディア鍵(Km)とを用いて検証する。この結果、署名の正当性の検証がNGとなる場合はスイッチ213を開いてコンテンツを再生しない一方、署名の正当性がOKとなる場合にはスイッチ213を閉じてコンテンツを再生可能とする。

#### 【0062】

このように、本実施の形態に係る著作権保護システムに用いるCPS-2記録方式においては、記録装置100は媒体固有番号(MID)を用いて認証子(MAC)を生成して記録媒体120に記録すると共に、再生装置200においては媒体固有番号(MID)を用いて認証子(MAC)の正当性を確認することが可能となる。そして、認証子(MAC)が正当でない場合には、再生装置200はコンテンツを再生することができないために、コピー等の不正な行為によるコンテンツの利用を防止して、著作権保護を図ることが可能となる。また、再生装置200は、CRLを用いて不正な記録装置100を排除することもできる。

#### 【0063】

以上、本実施の形態に係る著作権保護システムに用いるCPS-2記録方式の説明である。次に、本発明に係る記録装置100と著作権保護システムについて説明を行う。

#### 【0064】

図3は、本発明に係る記録装置100が備える処理部を示すブロック図、及び記録装置100の記録メディア120へのコンテンツ記録システムを示す概略図である。尚、記録装置100は、例えばDVDレコーダーであり、本発明においては複数の著作権保護記録方式に対応可能な記録メディア120にコンテンツを記録することを特徴とする。

#### 【0065】

また、本実施の形態においては複数の著作権保護記録方式として、従来のCPRM記録方式、上述した本実施の形態に係るCPS-2記録方式、著作権保護を必要としないNon-CP記録方式という3つ記録方式を用いて説明を行うが、本発明に係る記録装置100は、これら3つの記録方式に限定されるものではなく、他の著作権保護記録方式を用いた複数の記録方式にも適用可能である。

#### 【0066】

記録装置100は、コンテンツの受信を行う受信部301、記録メディア120に対するコンテンツの記録方式を決定する制御部302、記録装置100に備えられるキーボード等のユーザ入力可能な入力部303、コンテンツ等の記録を行うメモリ部である記憶部304、及び記録メディア120の書き込み及び読み出しを行うR/W部305を含む。

#### 【0067】

受信部301は、ネット配信、デジタル放送、DVD等を介して暗号化コンテンツ300を受信する。また、制御部302は、R/W部305を介して記録メディア120がCPRM記録方式、CPS-2記録方式、又はNon-CP記録方式に対応可能かを特定する記録メディア特定部302a、受信したコンテンツが著作権保護対象のコンテンツか否かのソースの種別の判定を行うソース特定部302b、記録装置100が記録メディア120に行う著作権保護記録方式の選択をCPRM記録方式、CPS-2記録方式、Non-CP記録方式という3つから行う記録方式選択部302c、これら3つの記録方式の変換を行う記録方式変換部302dを備える。

#### 【0068】

入力部303は、キーボード等であり、記録装置100のユーザからのコンテ

ンツの記録メディア120への著作権保護記録方式の選択を制御部302に入力する。また、記憶部304は、受信部301が受信した暗号化コンテンツ300等を記憶するハードディスクである。

#### 【0069】

R/W部305は、制御部302からの著作権保護システムの記録方式の指示に従い記録メディア120へのコンテンツ等の書き込みを行う。具体的には、CPRM記録方式、CPS-2記録方式、及びNon-CP記録方式から選択される1つ又は複数の記録方式に従って受信部301において受信したコンテンツ等の情報を記録メディア120に書き込む処理を行う。また、R/W部305は、記録メディア120が鍵無効化データ(HKB)や媒体固有番号(MID)を有するかを読み込み記録メディア特定部302aに伝える。そして、記録方式選択部302cは、記録メディア特定部302aやソース特定部302bからの情報に従ってコンテンツの記録メディア120への記録方式を決定してR/W部305に伝え、R/W部305は当該記録方式でコンテンツを記録メディア120に記録する。

#### 【0070】

図4は、本発明に係る記録装置100における著作権保護記録方式の選択の説明図である。この図4に示す記録装置100は、図3に示す記録装置100と同じ装置とする。

#### 【0071】

記録装置100は、著作権保護システムに用いる複数のコンテンツの記録メディア41等への記録方式を選択して受信したコンテンツ等の情報の記録を行う装置である。

#### 【0072】

図4においては、記録メディアの種類は3種類であり、書き換え不可領域に媒体固有情報(MID)及び鍵無効化データ(HKB)が書き込まれている記録メディア41、書き換え不可領域に媒体固有番号(MID)が書き込まれ鍵無効化データ(HKB)の書き込みがない記録メディア42、及び媒体固有情報(MID)と鍵無効化データ(HKB)とが共に書き込まれていない記録メディア43

となる。

#### 【0073】

このため、記録メディア41は、媒体固有情報(MID)と鍵無効化情報(HKB)を必要とするCPRM記録方式、媒体固有情報(MID)を必要とするCPS-2記録方式、及び著作権保護を行わないNon-CP記録方式の3つの著作権保護記録方式に対応可能となり、記録メディア42は、媒体固有情報(MID)を必要とするCPS-2記録方式、及び著作権保護を行わないNon-CP記録方式の2つの著作権保護記録方式に対応可能となり、記録メディア43は、Non-CP記録方式にのみ対応可能となる。従って、記録装置100の記録方式選択部302cは、記録メディア41等の種別に応じてコンテンツの記録方式を選択することが可能となる。尚、記録装置100からコンテンツの記録メディアへの記録不可の場合をNGとして示している。

#### 【0074】

図5は、本発明に係る記録装置100において記録メディアとソースとの種類から記録方式を特定するためのテーブルの一例を示す図である。このテーブルは記録装置100の記憶部304に書き換え可能に保持される。

#### 【0075】

図5においては、記録装置100は、記録メディアの種類が書き込み不可領域に媒体固有番号(MID)及び鍵無効化データ(HKB)が書き込まれている場合の記録メディア41であり、受信するソースの種類がネット配信の場合においては、記録装置100はCPRM記録方式、CPS-2記録方式、及びNon-CP記録方式の3つの記録方式から記録メディア41へのコンテンツの記録方式が選択されることを示している。

#### 【0076】

また、記録メディアが媒体固有情報(MID)及び鍵無効化データ(HKB)の書き込みのない記録メディア43の種類である場合においては、再生装置200側においてコンテンツの正当性を確認できないためにソースの種類に関わらずNon-CP記録方式のみが選択可能であることを示している。

(1枚目: アイデアの展開)

尚、本実施の形態に用いられる記録装置 100 よりコンテンツが記録される記録メディア 120 は DVD 以外に、CD-R/RW、将来の利用が予測される BD (Blu-ray Disc) 等も考え得る。

#### 【0077】

また、記録装置 100 における著作権保護記録方式の選択は、基本的には記録装置 100 側が決定する以外にも、コンテンツのプロバイダ側よりコンテンツにフラグ等を立てることにより指示を行い、記録装置 100 はこの指示に従った記録方式においてコンテンツの記録メディア 120 への記録を行う形式、記録装置 100 のユーザが記録装置 100 の機能に応じてキーボード等の入力部 303 を介して複数の記録方式の中より選択を行う形式も考え得る。

#### 【0078】

さらに、複数の著作権保護記録方式がある場合においては、各々の記録方式にセキュリティレベルの違いがあり、記録装置 100 は、送信されるコンテンツのセキュリティレベル、品質等に応じて記録方式を選択するような場合も想定される。

#### 【0079】

そして、暗号化コンテンツ 300 の取得を行う記録装置 100 が、放送、インターネット、CATV、DVD (Pre-recorded DVD (販売コンテンツ) や DVD-RAM (自己録コンテンツ)) 等の複数の入力チャネルを有する場合においては、入力チャネルの種類に応じて記録方式を選択するようなことも考え得る。

#### 【0080】

また、例えば、本発明に係る記録装置 100 が、CPRM 記録方式及び CPS-2 記録方式の 2 種類の著作権保護記録方式に対応している場合において、記録メディア 120 に CPRM 記録方式で記録されているコンテンツを、記録方式変換部 302 d において CPS-2 記録方式に変換して再記録することも可能となる。また、このように、記録装置 100 は、コンテンツをある記録方式から別の記録方式に変換するのみでなく、元の記録方式を残したまま新たな別の記録方式を追加して記録メディア 120 に記録することも考え得る。従って、1つのコン

テンツをCPRM記録方式及びCPS-2記録方式の両方で記録することにより、どちらか一方の記録方式にのみ対応している再生装置200においてもコンテンツを記録した記録メディア120の利用を図ることが可能となる。

#### 【0081】

図6は、本実施の形態に係る著作権保護システムの説明図である。サーバ装置600は、ネット配信、放送、DVD等の様々なソースからコンテンツを受信する。このサーバ装置600は一般的なサーバ装置や家庭内サーバ装置となる。

#### 【0082】

本図において、記録装置607等からコンテンツが記録される記録メディアは、例えばDVD-RAMディスクであり、CPRM記録方式とCPS-2記録方式の両方の記録方式をサポート可能となる。従って、これらの記録メディア610、611及び612は1枚で複数の著作権保護システムに対応可能なマルチディスクとなる。また、本実施の形態に係るコンテンツ配信元のサーバ装置600は、配信先の記録装置の能力、及び記録する記録メディアの種類に応じてコンテンツの配信を行うことをも特徴とする。尚、従来は1枚の記録メディアは単一の著作権保護システムに対応する記録メディアであり、複数の著作権保護システムに対応するマルチディスクを利用したコンテンツの移動やコピーを実現するものはない。

#### 【0083】

サーバ装置600は、3種類の記録装置607、記録装置608、及び記録装置609とネットワークを介して接続されている。記録装置607は、CPRM対応であり、記録装置608は、CPS-2対応であり、記録装置609は、CPRM/CPS-2の両方に対応可能な記録装置となる。

#### 【0084】

そして、サーバ装置600は、暗号化コンテンツの受信を行う受信部601、受信したコンテンツ等を記憶する記憶部602、サーバ装置600の製造時に書き込まれる機器固有情報を保持する機器固有情報保持部603、機器固有情報、鍵無効化データ等を用いてコンテンツの暗号化を行う暗号化部604、コンテンツの配信先の記録装置の能力、及び記録メディアの種類に合わせてコンテンツの

暗号化方式を選択する選択部 605、及び暗号化コンテンツを記録装置 607 等に配信する配信部 606 を含む。

#### 【0085】

まず、記録装置 607 が CPRM 対応である場合においては、選択部 605 は配布するコンテンツをセッション鍵で暗号化して配布することを選択する。そして、サーバ装置 600 は、暗号化部 604 において機器固有情報で暗号化されたコンテンツを機器固有情報保持部 603 より取得した機器固有情報を用いて復号化する。次に、サーバ装置 600 と記録装置 607 とが互いに認証処理を行ってセッション鍵を共有して、このセッション鍵で前記復号化したコンテンツの暗号化を行い配信部 606 を介して記録装置 607 へ送信する。

#### 【0086】

そして、記録装置 608 が CPS-2 対応である場合においては、選択部 605 は配布するコンテンツを鍵無効化データ (HKB) で暗号化して配布することを選択する。そして、サーバ装置 600 は、暗号化部 604 においてコンテンツを鍵無効化データ (HKB) に基づいて暗号化して配信部 606 を介して記録装置 608 へ送信する。

#### 【0087】

記録装置 609 が CPRM/CPS-2 対応である場合においては、選択部 605 は配布するコンテンツをセッション鍵又は鍵無効化データ (HKB) で暗号化して配布することを選択する。そして、サーバ装置 600 は、暗号化部 604 においてコンテンツをセッション鍵又は鍵無効化データ (HKB) に基づいて暗号化して配信部 606 を介して記録装置 609 へ送信する。

#### 【0088】

このように、本実施の形態に係る著作権保護システムにおいては、サーバ装置 600 は、暗号化コンテンツを記録装置に送信する際に、コンテンツの配布先の記録装置の能力、又は記録メディアの種別に応じてコンテンツの暗号化方法を選択することが可能となり、より効率的なコンテンツ配信を実現する。

#### 【0089】

また、本実施の形態に係る著作権保護システムにより、従来の単一の CPS 対



応ディスクのみでなく、今後登場が予測される複数の著作権保護記録方式対応のマルチディスクを利用したコンテンツの移動／コピーにおいても、著作権保護を図りつつ、より効率的なコンテンツの配信を行うことが可能となる。

#### 【0090】

図7は、コンテンツ配信先の記録装置のタイプとコンテンツの暗号化方式との関係を示す図である。尚、このテーブルは、サーバ装置600の記憶部602に書き込み可能に記憶されるものである。また、この図7に示すテーブルは一例であり、本発明はこれに限定されるものではない。

#### 【0091】

CPRM対応記録装置(607)においては、サーバ装置600から記録装置607に配信されるコンテンツの暗号化方式にはセッション鍵が用いられ、CPS-2対応記録装置(608)においては、サーバ装置600から配信されるコンテンツの暗号化方式には鍵無効化データ(HKB)が用いられ、CPRM/CPS-2対応記録装置609においては、サーバ装置600から配信されるコンテンツの暗号化方式にはセッション鍵又は鍵無効化データ(HKB)の両方を用いることが可能であることを示す。尚、CPS-2対応の場合であっても、セッション鍵で送る構成とすることも考え得る。

#### 【0092】

尚、図6においては、記録装置607等が記録メディア610等の書き込み不可領域に書き込まれている媒体固有番号(MID)を読み込んだ後に、この媒体固有番号をサーバ装置600に送信して、サーバ装置600側が認証子(MAC)を生成して記録装置607等に送信する構成でも良い。

#### 【0093】

また、記録装置607等が複数の著作権保護システムに対応する場合には、記録装置607等のユーザがサーバ装置600の配信するコンテンツの暗号化の形態を指定することができる構成でも良い。また、サーバ装置600の管理者が指定してもよい。

#### 【0094】

さらに、サーバ装置600は、コンテンツの記憶部602への蓄積形態と、記



録装置 607 等から指定されるコンテンツの暗号化形態が異なる場合は、記録装置 607 等からの指定に従い配信するコンテンツの再暗号化を施す構成でも良い。

#### 【0095】

次に、記録装置 100 における著作権保護システムの記録方式の選択における動作について説明する。図 8 は、本発明に係る記録装置 100 におけるコンテンツの記録メディア 120 への記録方式の選択手順を示すフローチャートである。

#### 【0096】

まず、記録装置 100 は、コンテンツを受信してネット配信、DVD 等のソースの種類から記録方式の指定、著作権保護コンテンツか否か、又は記録メディアを読み込んで記録メディア 120 の種類よりコンテンツの記録メディア 120 への記録方式が指定されるか否か確認する (S801)。この指定が行われる場合においては (S801 で Y)、指定された記録方式に決定する (S806)。

#### 【0097】

次に、指定がされない場合には (S801 で N)、記録装置 100 は、キーボード等の入力部 303 を介してユーザがコンテンツの記録メディア 120 への記録方式を指定しているか否か確認する (S802)。そして、指定される場合には (S802 で Y)、指定された記録方式に決定する (S806)。指定されない場合においては (S802 で N)、記録装置 100 はネット配信、DVD、放送等のソースの種類を判定する (S803)。

#### 【0098】

次に、記録装置 100 は、記録メディア 120 を読み込むことにより記録メディア 120 の種類に対応する著作権保護システムを判定する (S804)。そして、記録装置 100 は、メディアの種別、ソースの種別に応じてコンテンツの記録メディア 120 への記録方式を決定するために、上述の図 5 に示すテーブルを参照して記録方式の決定を行う (S805)。

#### 【0099】

従って、本発明の記録装置 100 は、複数の著作権保護システムの記録方式の内、記録装置 100 の能力、及び記録メディア 120 の種類に応じて最適の記録

方式を1つ又は複数選択することができ、複数の著作権保護システムに対応可能な記録装置100とすることが可能となる。

#### 【0100】

図9は、サーバ装置600において、記録装置607等に配信するコンテンツの暗号化方式を決定する場合の手順を示すフローチャートである。

まず、サーバ装置600は、コンテンツの配信先の相手の記録装置607等のタイプの特定を行う。具体的には、図7に示すようにCPRM対応、CPS-2対応、又はCPRM/CPS-2対応かの特定を行う(S901)。

#### 【0101】

次に、サーバ装置600は、図7に示すテーブルを参照してコンテンツの暗号化方式の決定を行う(S902)。そして、サーバ装置600は配信するコンテンツを決定された暗号化方式に従って暗号化して(S903)、配信部606を介して配信コンテンツの出力を行う(S904)。

#### 【0102】

このため、コンテンツ配信元であるサーバ装置600が、配信先の記録装置607等の能力に応じてコンテンツの配信を行うことが可能となり、複数の記録方式に対応可能に、より効率的なコンテンツ配信を実現できる。

#### 【0103】

図10は、本実施の形態に係る著作権保護記録方式であるCPS-2記録方式を用いて記録されたコンテンツのリモート再生及びコピーにおける不正使用を説明するための参考図である。

#### 【0104】

図10において、AVCサーバ1002は、例えば家庭内のサーバ装置であり、無線等によりリモート端末機器1003に暗号化コンテンツの配信を行うものである。尚、図10(a)は正規のリモート再生を説明し、図10(b)は、記録メディア1001のコピー等を行った不正な記録メディア1004を用いて不正にコンテンツのリモート再生を図る場合を説明するものである。

#### 【0105】

記録メディア1001は、書き込み不可領域に記録メディア毎に固有の番号で

ある媒体固有番号 (MID)、書き込み可能領域に認証子 (MAC)、署名、鍵無効化データ (HKB)、コンテンツが書き込まれている。AVCサーバ1002は、リモート端末機器1003に媒体固有番号 (MID)、認証子 (MAC)、署名を送信して、リモート端末機器1003は、コンテンツの不正使用がないかの検証を行う。また、リモート端末機器1003は、AVCサーバ1002より送信される鍵無効化データ (HKB) 及びコンテンツを受信して、コンテンツの復号化、再生を行う。

#### 【0106】

一方、不正にコピーを行った記録メディア1004を用いてコンテンツの利用を行う場合においては、通常は記録メディア毎の製造時における媒体固有番号 (MID) が異なるために、CPS-2記録方式においては、コンテンツの不正使用を防止することが可能となる。しかし、図10(b)においては、媒体固有番号 (MID) の配信を無線等を用いたリモート再生により行っているために、媒体固有番号 (MID) が通信路上において正規の媒体固有番号に書き換えられる可能性が考えられる。このような場合においては、AVCサーバ1005からリモート再生端末1006に送ったコンテンツを不正に利用されてしまう可能性がある。すなわち、CPS-2記録方式により記録メディア1004に記録されるコンテンツは、家庭内のリモート再生等において行う場合においては、媒体固有番号 (MID) を無線上で不正取得するアタックが考え得る。

#### 【0107】

このような問題を解決するために、本実施の形態においては通信路上にSAC (Secure Authentication Channel) を張って通信路の安全を図ることとする。図11は、本実施の形態に係るCPS-2記録方式を用いたコンテンツのリモート再生及びリモート記録を行う場合の全体図である。

#### 【0108】

図11(a)においては、図10(b)に示す媒体固有番号 (MID) が通信路上にて書き換えられることを防止するために暗号化通信路 (SAC) を張った後に、媒体固有番号 (MID)、認証子 (MAC)、及び署名をAVCサーバ1102からリモート再生装置1103に送信している。

## 【0109】

また、図11(b)においては、PC/AVCサーバ1105からリモート記録装置1106にコンテンツの送信を行う場合の説明図であり、記録メディアの媒体固有番号(MID)に対応する情報としてハードディスク1104の識別番号となるHDD IDを用いている。そして、図11(a)に示す場合と同様に通信路をSAC等により暗号化通信路とした後に、PC/AVCサーバ1105は、HDD ID、認証子(MAC)、及び署名をリモート記録装置1106に送信する。尚、この場合においては、認証子(MAC)はHDD IDを用いてPC/AVCサーバ1105において生成される。

## 【0110】

従って、本実施の形態においては、暗号化通信路(SAC)を用いることによりHDD IDを通信路上にて置き換えられないように安全にリモート記録装置1106側に送信することが可能となり、リモート記録装置1106は、鍵無効化データ(HKB)、コンテンツをそのまま記録メディア1107に記録すると共に、記録メディア1107より媒体固有番号(MID)を読み出して、この媒体固有番号に対応する認証子(MAC)、及び署名を生成した後に認証子(MAC)及び署名を記録メディア1107に記録する。このようにリモート記録装置1106は検証処理と生成処理とを行う必要がある。

## 【0111】

尚、図11において、PC/AVCサーバ1105からリモート記録装置1106に送信されるHDD IDの代わりにPCやPCアプリのIDを用いることも考え得る。また、リモート記録装置1106がPC/AVCサーバ1105を別途認証するような通信においてはHDD ID、認証子(MAC)、及び署名の送信は行う必要がなく、さらに、DVDダブルドライブのような記録装置において記録を行う場合においては暗号化通信路(SAC)とする必要がないことは言うまでもない。

## 【0112】

このように、リモート端末機器1103等にコンテンツ配信を行う場合においても、通信路を暗号化通信路(SAC)とすることにより、不正なサーバ装置は

暗号化通信路 (SAC) を張ることができず、媒体固有情報 (MID) や HDD ID の通信路上での書き換えを防止して、安全にリモート端末機器 1103 及びリモート記録機器 1106 にコンテンツ配信を行うことが可能となる。

#### 【0113】

尚、上述した実施の形態においては、著作権保護システムに用いるコンテンツ等の記録方式として CPRM 記録方式、CPS-2 記録方式、及び Non-CP 記録方式を用いて説明を行ったが、本発明に用いることにできる著作権保護記録方式はこれに限定されるものではない。すなわち、本発明において記録装置 100 は、複数の著作権保護システムに対応可能にコンテンツの記録メディアへの記録を行うことができる。

#### 【0114】

##### 【発明の効果】

以上の説明から明らかなように、本発明に係る記録装置は、デジタル著作物であるコンテンツを記録媒体に記録する記録装置であって、外部から提供されるコンテンツを取得するコンテンツ取得手段と、受信されたコンテンツの種別を特定するコンテンツ種別特定手段と、前記記録媒体の種別を特定する記録媒体種別特定手段と、前記コンテンツ種別特定手段で特定されたコンテンツの種別と前記記録媒体種別特定手段で特定された記録媒体の種別とに基づいて、複数の記録方式の中から少なくとも 1 つの記録方式を選択する記録方式選択手段と、選択された記録方式に従って前記記録媒体に前記コンテンツを記録する記録手段とを備えることを特徴とする。

#### 【0115】

これにより、記録装置は、複数の著作権保護記録方式から、記録媒体の種別、コンテンツの種別等に応じてコンテンツの記録媒体への記録方式を選択することが可能となる。

#### 【0116】

また、本発明に係る記録装置は、前記コンテンツ取得手段は、取得したコンテンツを、伝送路を介して前記記録手段に送信し、前記記録手段は、前記伝送路を介して受信したコンテンツを前記記録媒体に記録し、前記コンテンツ取得手段は

、前記コンテンツを、送信先となる記録手段が採用する記録方式に従って暗号化した後に、当該暗号化コンテンツを前記記録手段に送信することを特徴とする。

【0117】

このため、サーバ装置は、暗号化コンテンツを記録装置に送信する際に、コンテンツの配布先の記録装置、又は記録する記録メディアの種別に応じてコンテンツの配信方法を選択する。従って、コンテンツ配信元であるサーバ装置が、配信先の記録装置の能力、或いはコンテンツが記録される記録メディアの種類に応じてコンテンツの配信を行うことが可能となり、より効率的なコンテンツ配信を実現することができる。

【0118】

さらに、本発明に係る著作権保護システムは、伝送路を介して接続されたサーバ装置と端末装置とから構成される著作権保護システムであって、前記サーバ装置は、暗号化コンテンツを当該暗号化コンテンツを復号化するのに必要な復号化情報とが記録された記録媒体から前記暗号化コンテンツ及び前記復号化情報を読み出す読み出し手段と、読み出された暗号化コンテンツ及び復号化情報を前記伝送路を介して前記端末装置に送信する送信手段とを備え、前記端末装置は、前記伝送路を介して送信されてくる暗号化コンテンツ及び復号化情報を受信する受信手段と、受信された暗号化コンテンツを受信された復号化情報を用いて復号化する復号化手段とを備え、前記送信手段は、前記端末装置との間でセキュアな伝送チャネルを確立した後に、当該伝送チャネルを介して前記復号化情報を送信することを特徴とする。

【0119】

これにより、リモート端末機器にコンテンツ配信を行う場合において、通信路を暗号化通信路とすることにより、不正なサーバ装置は暗号化通信路を張ることができないために、媒体固有情報の通信路上での書き換えを防止して、安全にリモート端末機器側にコンテンツ配信を行うことが可能となる。

【図面の簡単な説明】

【図1】

本実施の形態に用いる著作権保護システムに用いるCPS-2記録方式の全体

構成を示す概略図である。

【図 2】

デバイス鍵 D K\_\_1 の再生装置が記録した記録媒体に格納されている各種データの具体例を示す図である。

【図 3】

記録装置が備える処理部を示すブロック図、及び記録装置の記録メディアへのコンテンツ記録システムを示す概略図である。

【図 4】

記録装置における著作権保護記録方式の選択の説明図である。

【図 5】

記録装置において記録メディアとソースとの種類から記録方式を特定するためのテーブルの一例を示す図である。

【図 6】

本実施の形態に係る著作権保護システムの説明図である。

【図 7】

コンテンツ配信先の記録装置のタイプとコンテンツの暗号化方式の関係を示す図である。

【図 8】

記録装置におけるコンテンツの記録メディアへの記録方式の選択手順を示すフローチャートである。

【図 9】

サーバ装置において、記録装置に配信するコンテンツの暗号化方式を決定する場合の手順を示すフローチャートである。

【図 10】

本実施の形態に係る著作権保護記録方式である C P S - 2 記録方式を用いて記録されたコンテンツのリモート再生及びコピーにおける不正使用を説明するための参考図である。

【図 11】

本実施の形態に係る C P S - 2 記録方式を用いたコンテンツのリモート再生及

びリモート記録を行う場合の全体図である。

【図 12】

従来の鍵無効化技術を説明するための説明図である。

【図 13】

従来の単一の著作権保護システムに対応する記録装置の説明図である。

【符号の説明】

- 100 記録装置
- 120 記録媒体
- 130 鍵無効化データ配信局
- 140 CRL 配信局
- 200 再生装置
- 301 受信部
- 302 制御部
  - 302a コンテンツ特定部
  - 302b ソース特定部
  - 302c 記録方式選択部
  - 302d 記録方式変換部
- 303 入力部
- 304 記憶部
- 305 R/W部
- 600 サーバ装置
  - 601 受信部
  - 602 記憶部
  - 603 機器固有情報保持部
  - 604 暗号化部
  - 605 選択部
  - 606 配信部
  - 607 CPRM対応記録装置
  - 608 CPS-2対応記録装置



6 0 9 C P R M / C P S - 2 対応記録装置

6 1 0 記録メディア

1 0 0 1 記録メディア

1 0 0 2 A V C サーバ

1 0 0 3 リモート端末機器

1 1 0 1 記録メディア

1 1 0 4 ハードディスク

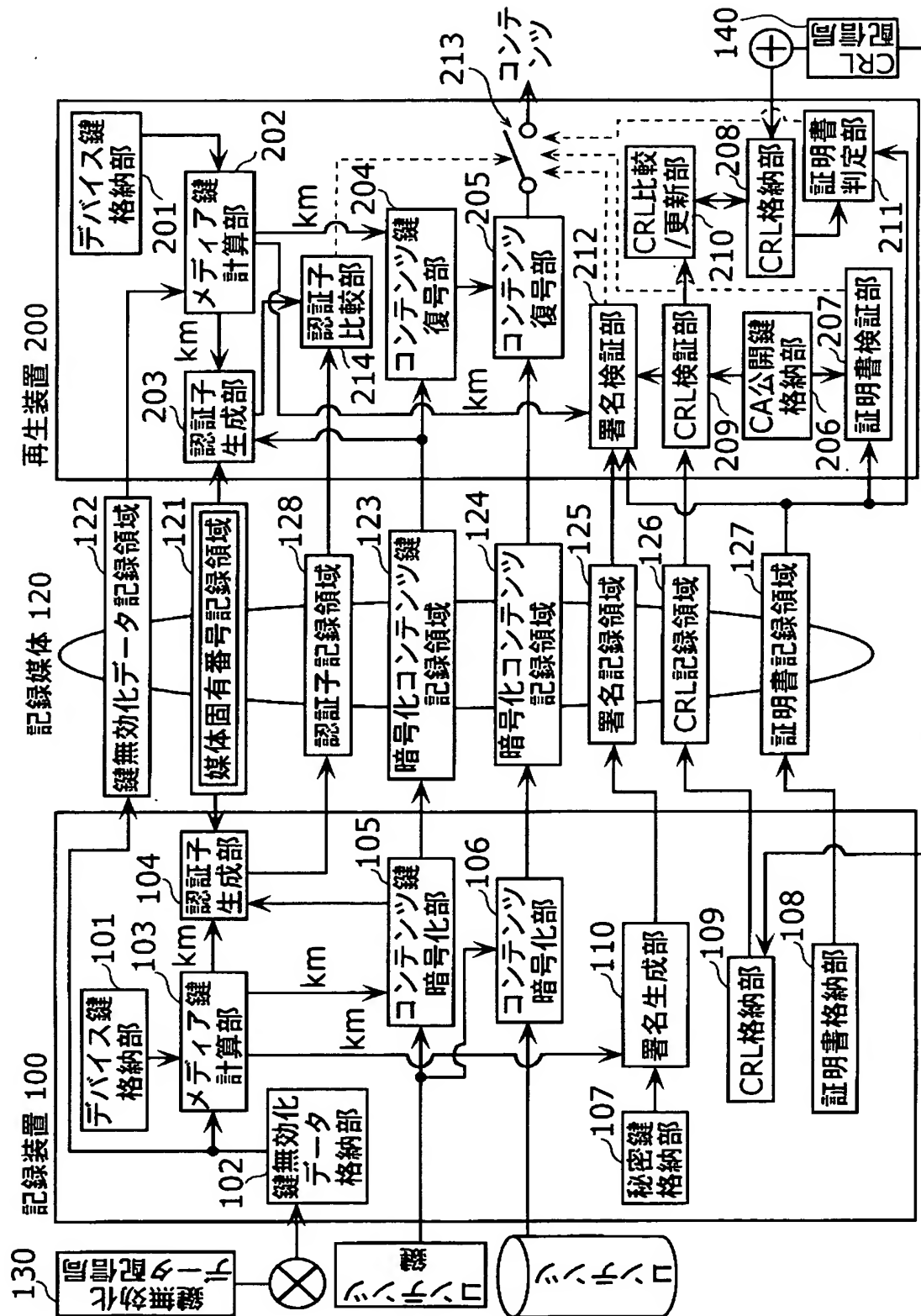
1 1 0 5 P C / A V C サーバ

1 1 0 6 リモート記録機器

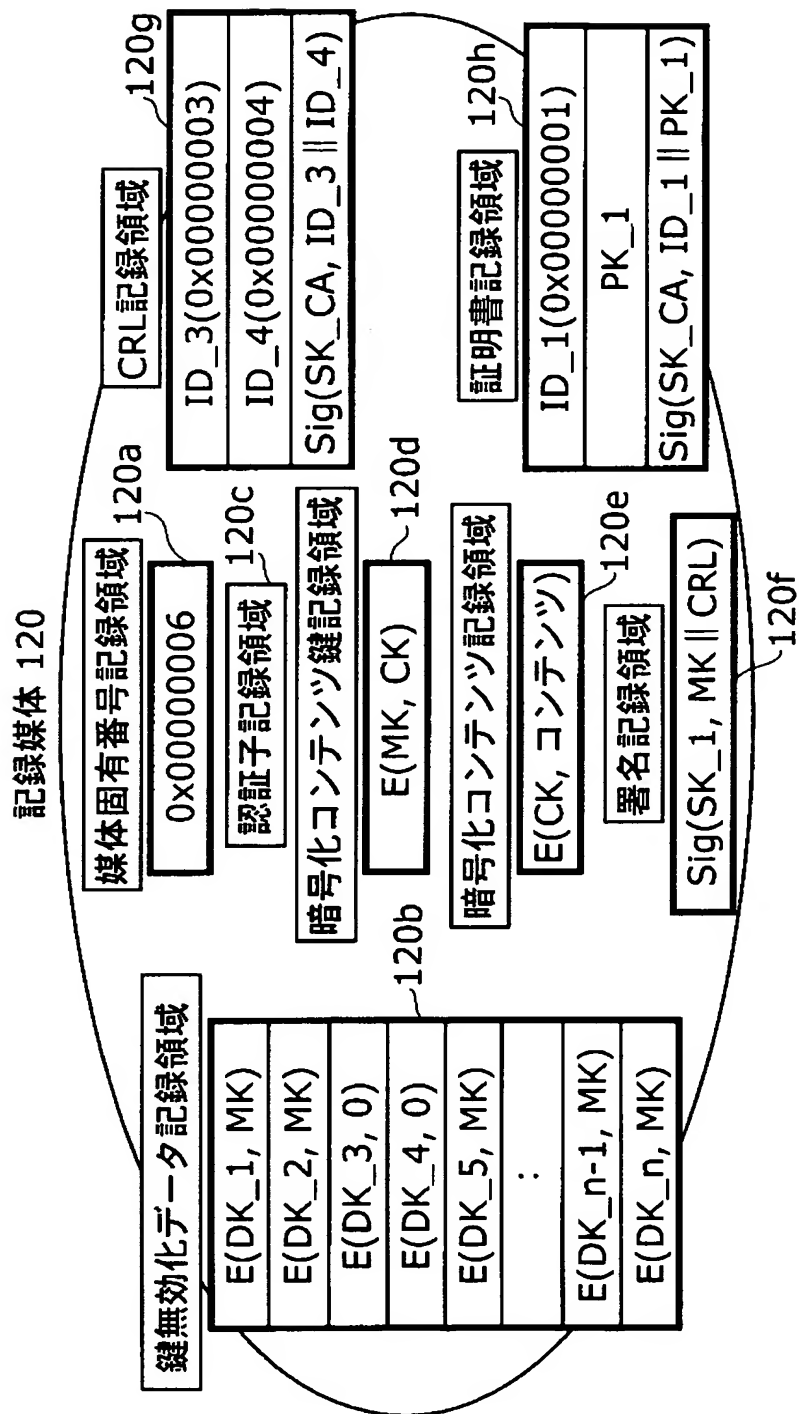
1 1 0 7 記録メディア

【書類名】 図面

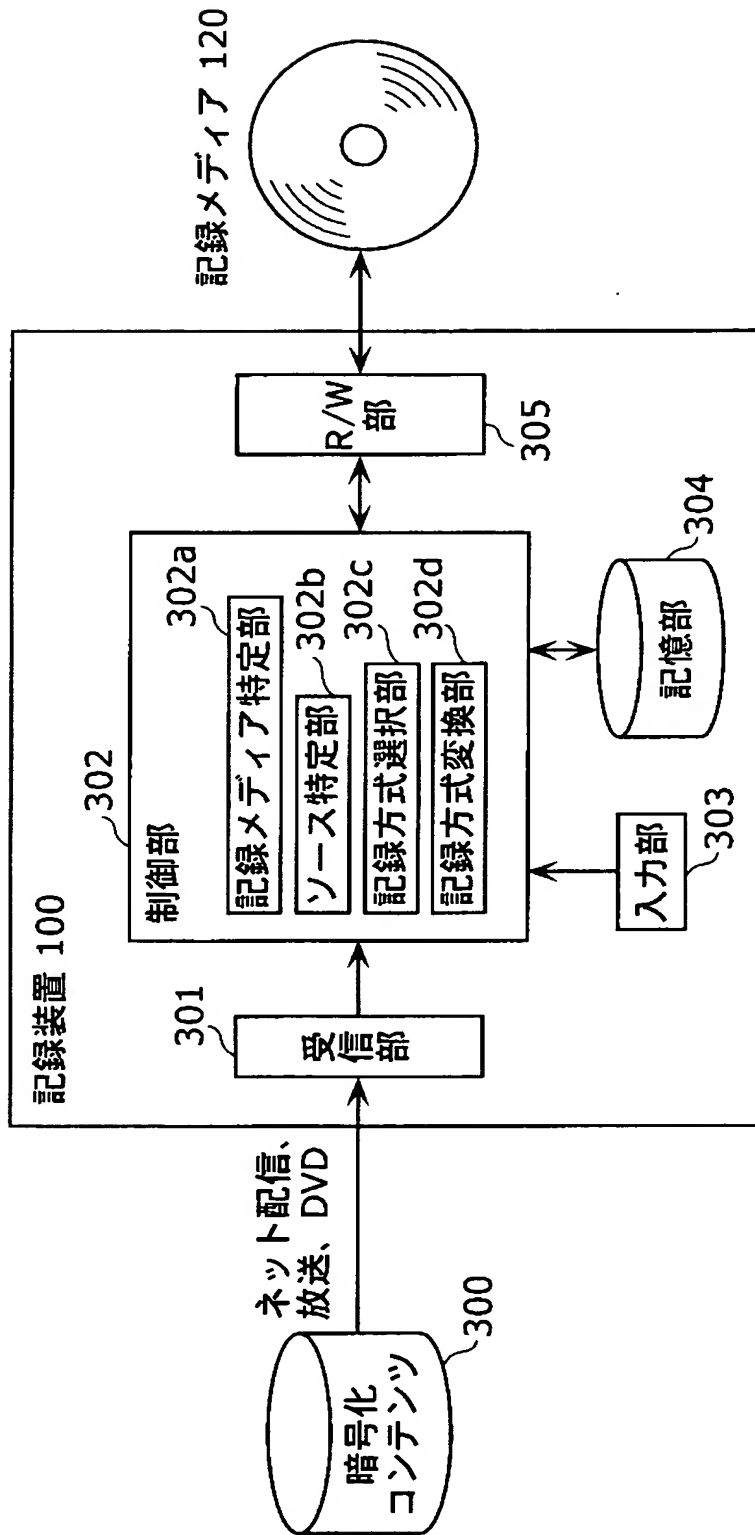
【図 1】



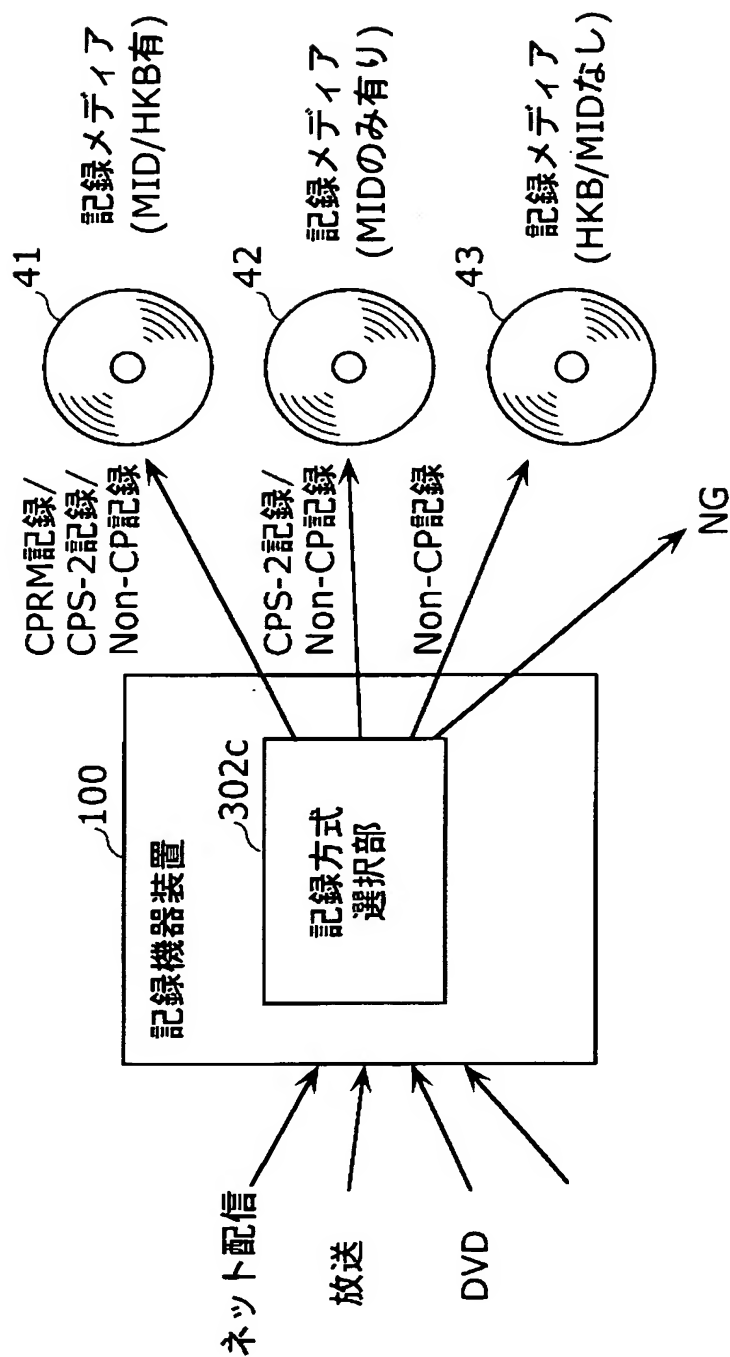
【図 2】



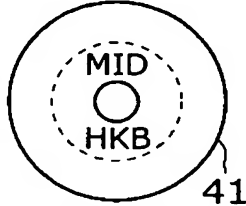
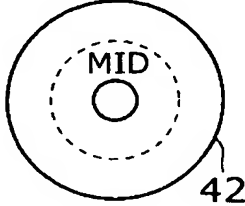
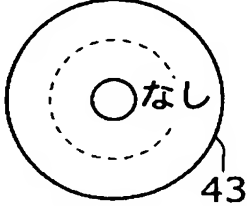
【図 3】



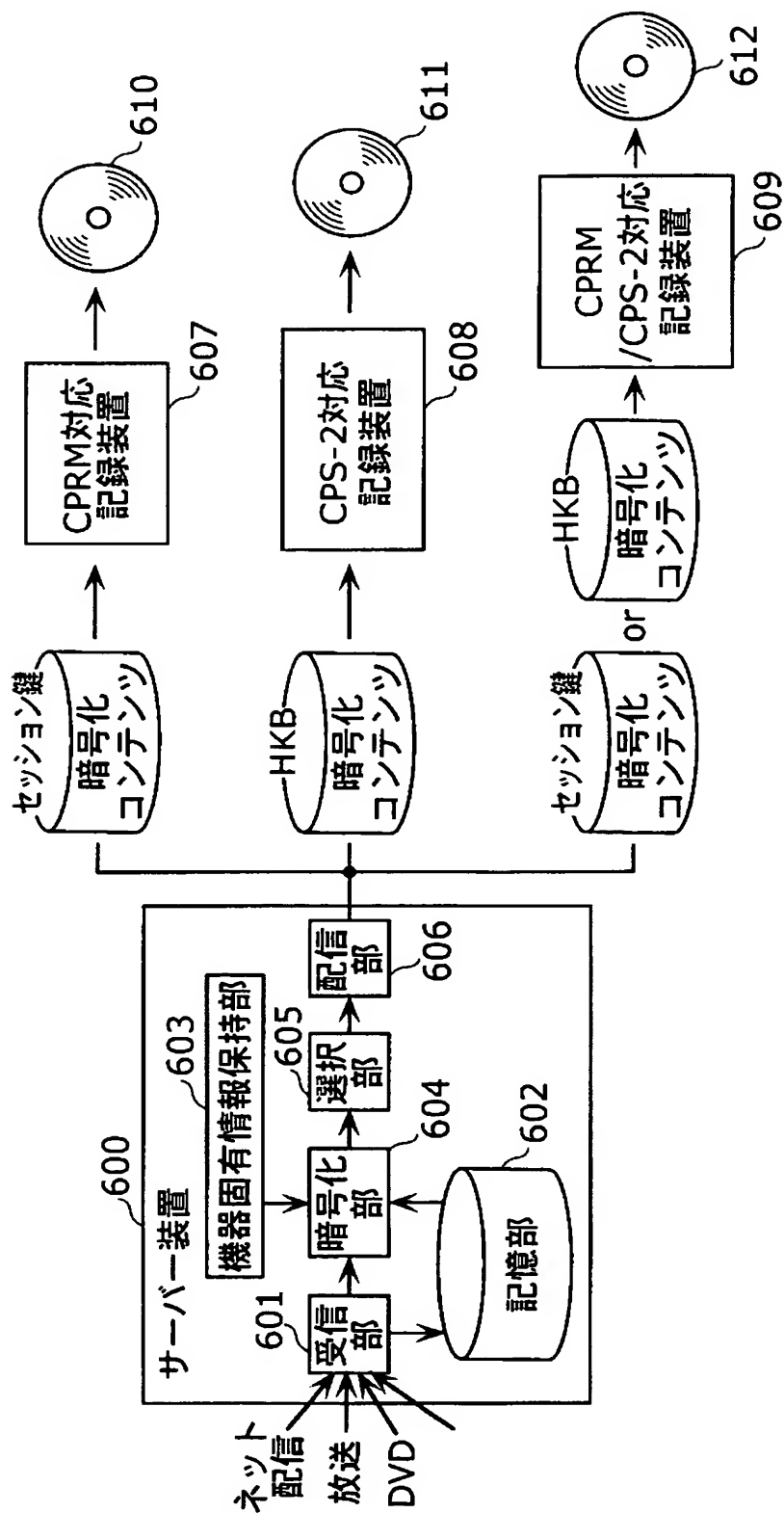
【図 4】



【図 5】

記録 メディア ソース			
ネット配信	CPRM記録/ CPS-2記録/ Non-CP記録	CPS-2記録/ Non-CP記録	Non-CP記録
DVD	CPS-2記録/ Non-CP記録	CPS-2記録	Non-CP記録
放送	CPRM記録/ CPS-2記録	Non-CP記録	Non-CP記録
⋮			

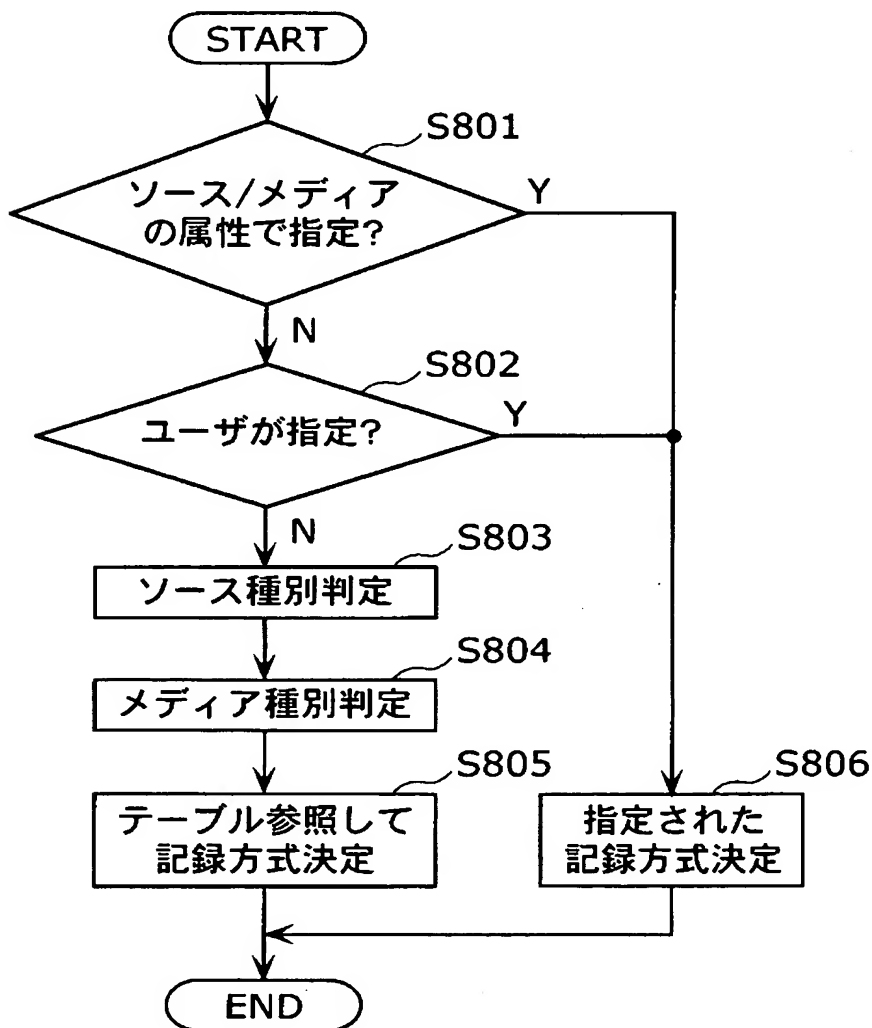
【図 6】



【図 7】

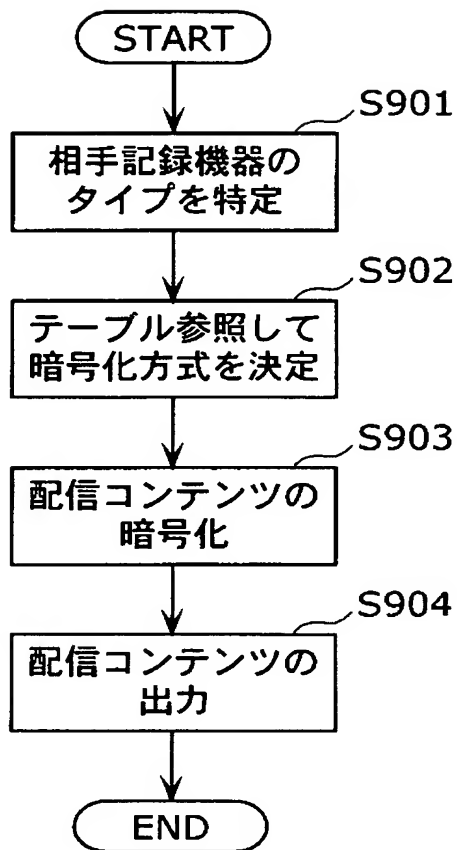
コンテンツ配信先の 記録機器 のタイプ 暗号化方式	CPRM対応 記録装置 (607)	CPS-2対応 記録装置 (608)	CPRM/ CPS-2対応 記録装置 (609)
セッション鍵	○	×	○
鍵無効化データ (HKB)	×	○	○

【図 8】

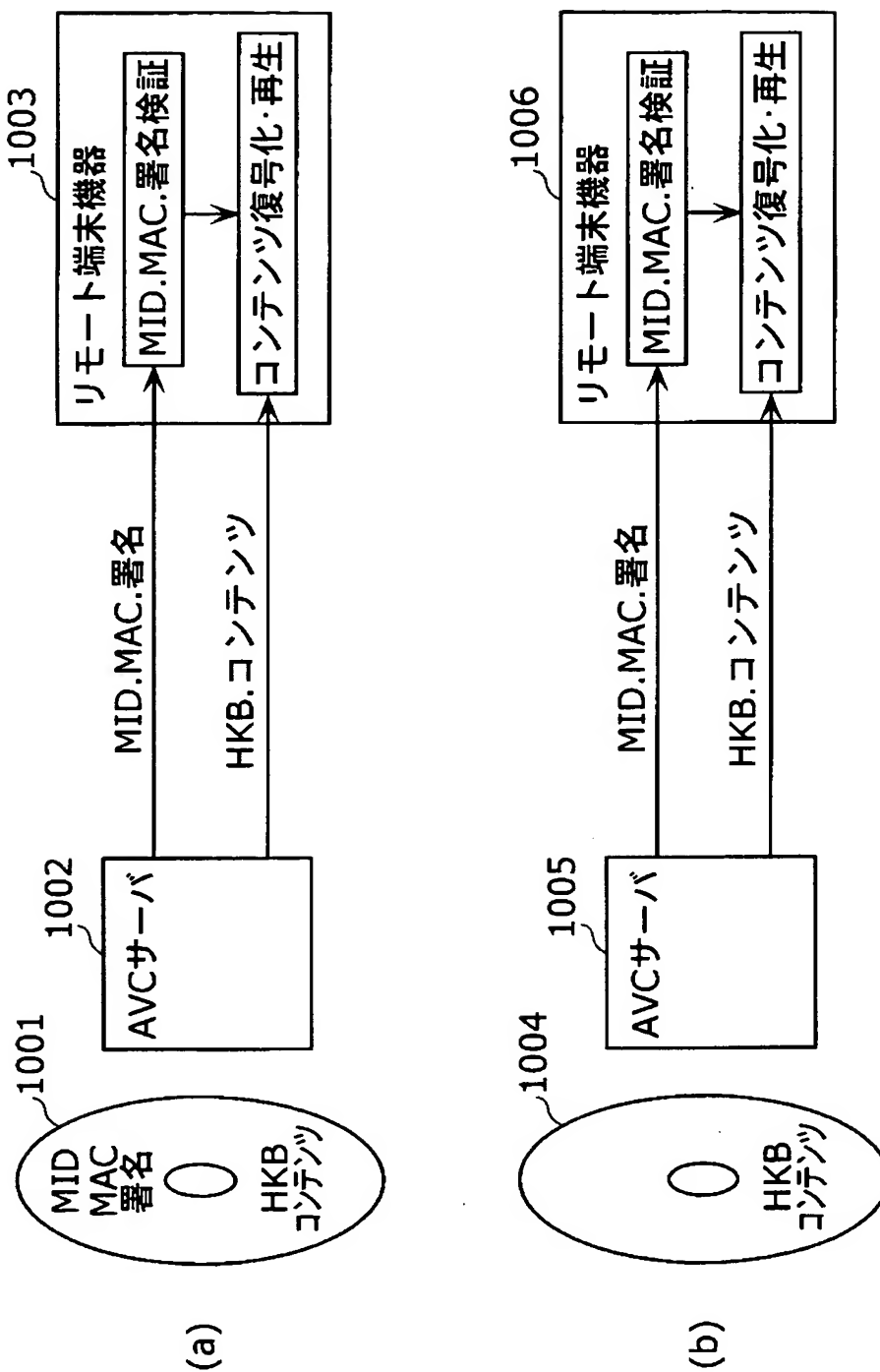




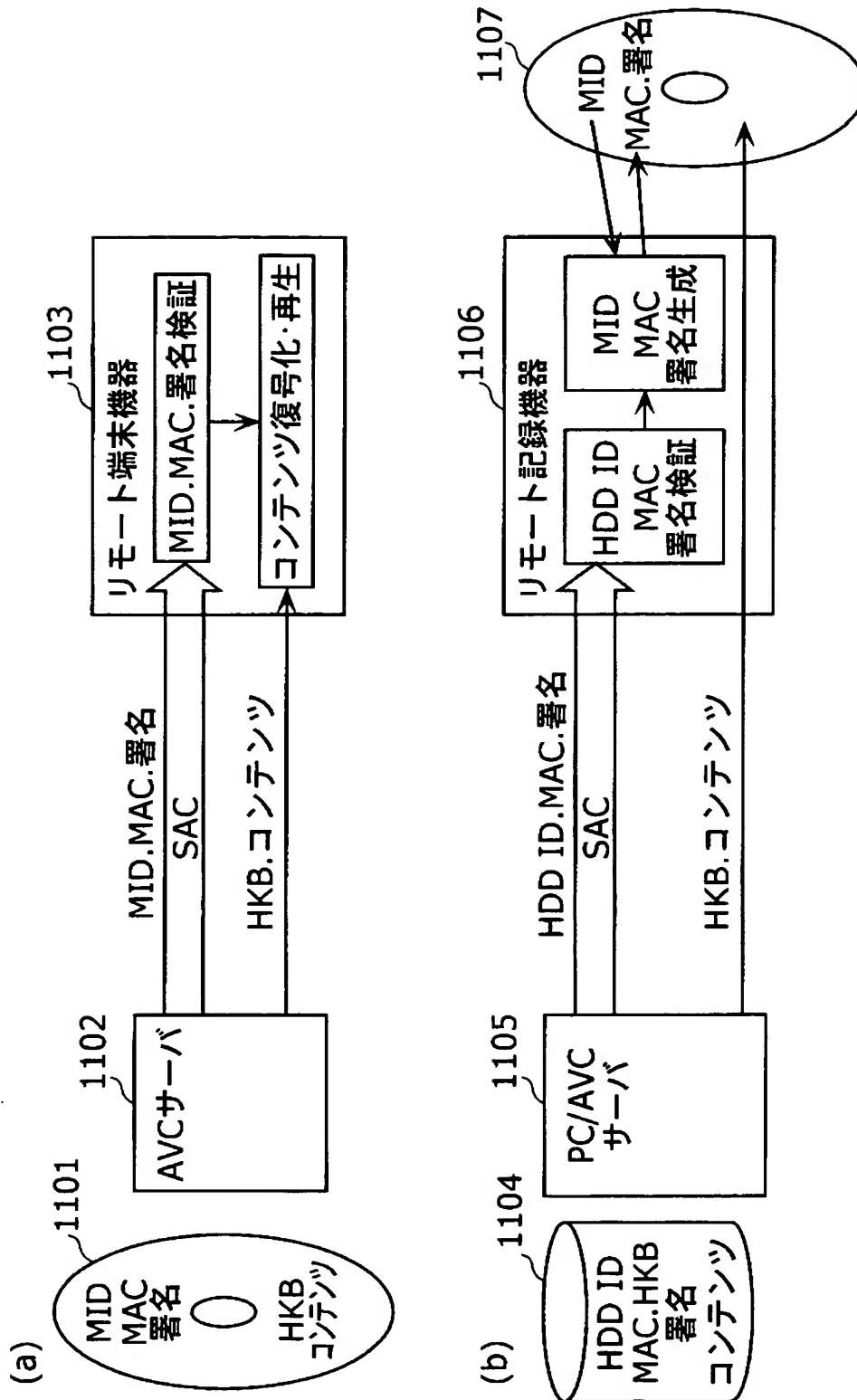
【図 9】



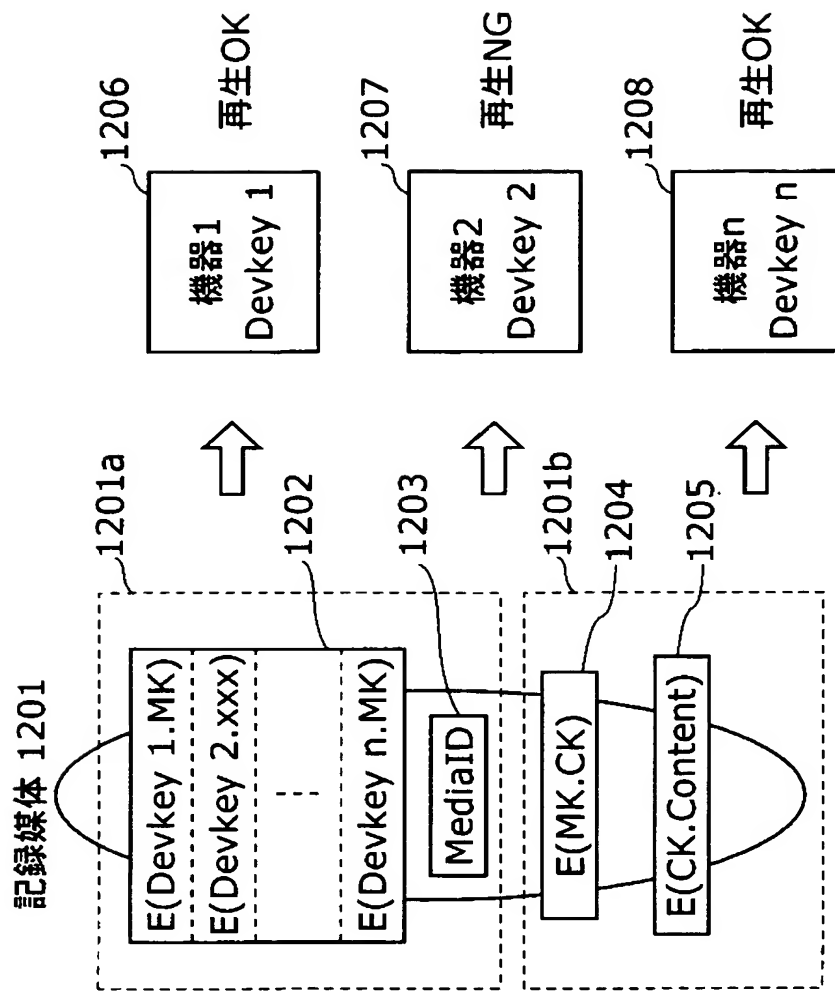
【図10】



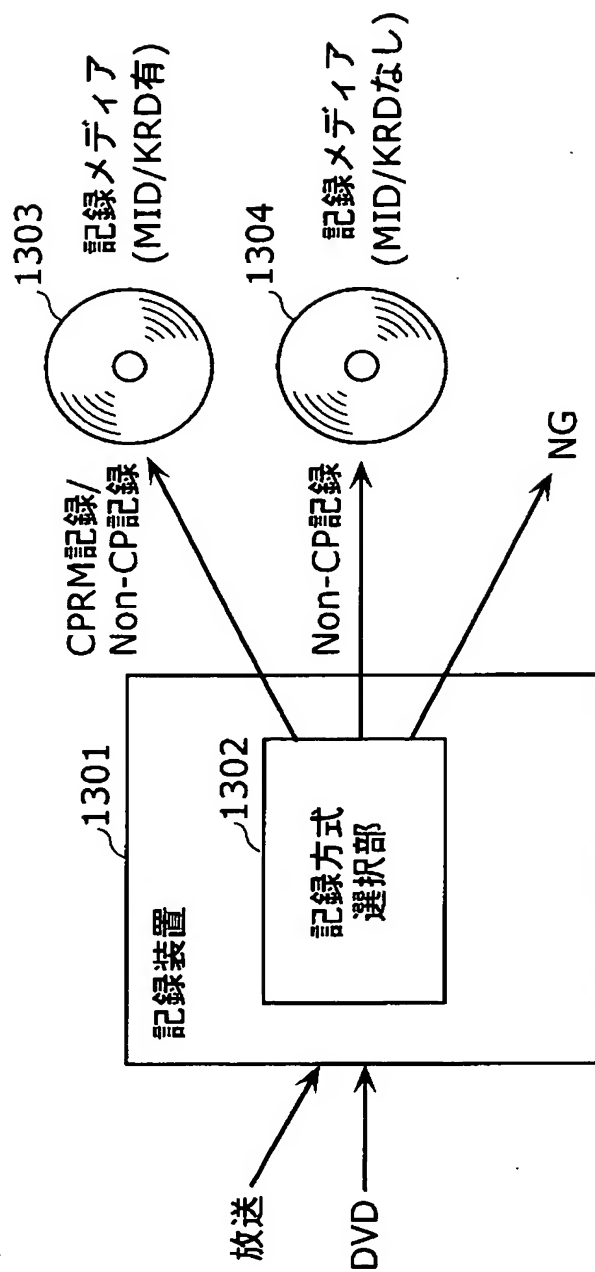
【図 11】



【図 12】



【図 13】



【書類名】 要約書

【要約】

【課題】 コンテンツを記録媒体に記録する記録装置において、複数の著作権保護記録方式に対応可能な記録装置を提供する。

【解決手段】 記録装置 100 は、コンテンツの受信を行う受信部 301、記録メディア 120 に対するコンテンツの記録方式を決定する制御部 302、記録メディアの書き込み及び読み出しを行う R/W部 305 を備え、前記制御部 302 は、前記 R/W部 305 を介して記録メディアの種類を特定する記録メディア特定部 302a、受信したコンテンツが著作権保護対象のコンテンツか否かのソースの種別の判定を行うソース特定部 302b、記録メディア 120 へのコンテンツの記録方式の選択を行う記録方式選択部 302c、記録方式の変換を行う記録方式変換部 302d を備える。

【選択図】 図 3

認定・付加情報

特許出願の番号	特願 2 0 0 3 - 0 8 1 4 6 7
受付番号	5 0 3 0 0 4 7 5 7 2 7
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 5 年 4 月 4 日

< 認定情報・付加情報 >

【提出日】 平成15年 3月24日

次頁無

特願 2 0 0 3 - 0 8 1 4 6 7

出 願 人 履 歷 情 報

識別番号

[ 0 0 0 0 0 5 8 2 1 ]

1 . 変 更 年 月 日

1 9 9 0 年    8 月 2 8 日

[ 変 更 理 由 ]

新 規 登 録

住    所

大 阪 府 門 真 市 大 字 門 真 1 0 0 6 番 地

氏    名

松 下 電 器 産 業 株 式 会 社